



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/933,760	08/22/2001	Timothy C. Williams	P62141US1	6977

136 7590 06/16/2004

JACOBSON HOLMAN PLLC
400 SEVENTH STREET N.W.
SUITE 600
WASHINGTON, DC 20004

EXAMINER

KIM, JUNG W

ART UNIT PAPER NUMBER

2132

DATE MAILED: 06/16/2004

13

Please find below and/or attached an Office communication concerning this application or proceeding.

SL

Office Action Summary

Application No.

09/933,760

Applicant(s)

WILLIAMS, TIMOTHY C.

Examiner

Jung W Kim

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 April 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 25-32, 34, 37-45, 47, 49, 54, 59, 69-71, 73-75 and 85-89 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 25-32, 34, 37-45, 47, 49, 54, 59, 69-71, 73-75 and 85-89 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. Claims 25-32, 34, 37-45, 47, 49, 54, 59, 69-71, 73-75, and 85-89 have been examined. Applicant has canceled claims 35-36, 48, 50-53, 55-58, 60-68, 72, and 76-84, and added new claims 85-89 in the amendment filed on April 16, 2004.

Response to Amendment

2. The objection to claim 36 is withdrawn since the claim has been canceled.
3. The rejections to claims 66 and 82 under 35 U.S.C. 112, second paragraph are withdrawn since the claims have been canceled.
4. The rejections to claims 54 and 73 under 35 U.S.C. 112, second paragraph are withdrawn as the amendments to the claims overcome the rejections.

Response to Arguments

5. Applicant's arguments with respect to amended claims 25-32, 34, 37-45, 47, 49, 54, 59, 69-71, and 73-75 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

6. Claim 38 is objected to because of the following informalities: in claim 38, the word "security" is misspelled. Appropriate correction is required.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claim 49 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

9. Claim 49 recites the limitation "the destination". There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

11. Claims 25-27, 31, 34, 37-40, 44, 47, 49, 59, 69, 70-71, 74, and 85-87 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boyle et al. U.S. Patent No. 5,577,209 (hereinafter Boyle) in view of Garfinkel et al. Practical UNIX Security (hereinafter Garfinkel). As per claim 25, Boyle discloses a multi-level secure network having a plurality of host computers accessible to users and connected to a network

medium that has access to an untrusted line (see Boyle, Abstract; col. 2, lines 46-65),
the secure network comprising:

- a. a network security controller for generating a user profile for each user and for sending the user profile to security devices connected to the network medium, the user profile defining a plurality of destinations which the user is authorized to access through discretionary access control and mandatory access control security mechanisms, wherein a plurality of user profiles define virtual private networks of communication comprising subsets of host computers (see Boyle, col. 3, lines 30-42; col. 4, lines 27-30 and 45-53; col. 5, 33-65, especially lines 50-52; col. 6, lines 15-32; col. 8, lines 51-62, especially line 59; col. 9, lines 38-46; col. 10, lines 34-42; Figure 1 and related text); and
- b. security devices connected to the network medium for receiving the user profiles generated at the network security controller and for implementing security mechanisms associated with the user profiles, each security device associated with one host computer, each security device having an authorization device for authorizing users at the associated host computer, the security device permitting the authorized user, via the associated host computer, to select a user's profile associated with the user and for restricting access of the host computer to the destinations defined in the selected user's profile (see Boyle col. 5, lines 1-8; col. 7, line 46-col. 8, line 21, especially lines 47 and 51-52; col. 10, lines 31-42; Figures 1, 4A-F, and 6A).

12. Boyle does not expressly disclose that the network security controller generates a plurality of user profiles for a single user, wherein a single user selects a profile from the plurality of user profiles to access the restricted destinations. However, this feature is commonly integrated into systems that maintain discretionary and mandatory access controls on its users. For example, Garfinkel discloses a UNIX system wherein users are provided with one or more profiles and a user selects a profile by either logging in under a username associated with a particular profile, or using the 'su' command to switch from one profile to another; this one-to-many association enables a user to embrace multiple roles on the network-each profile corresponding to a certain role (see Garfinkel, page 22, 2nd paragraph; page 23, 2nd paragraph; page 46-47, 'User Identifiers' and 'Groups and Group Identifiers'; page 53, 'su(1) command'). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Garfinkel to the network disclosed by Boyle. Motivation for such an implementation enables a user to take on multiple roles as taught by Garfinkel. The aforementioned covers claim 25.

13. As per claim 26, Boyle covers a secure network as outlined above in the claim 25 rejection under 35 U.S.C. 103(a). In addition, the at least one destination comprises at least one other host computer of the network or the untrusted line (see Boyle, Figure 2, 'Bridge (SNIU)' and 'Gateway (SNIU)'; col. 5, lines 50-53; col. 6, lines 15-20).

14. As per claim 27, Boyle covers a secure network as outlined above in the claim 25 rejection under 35 U.S.C. 103(a). In addition, the security devices, when implementing security mechanisms, allows the host computer to connect to a trusted destination (see Boyle, col. 10, lines 30-59).

15. As per claim 31, Boyle covers a secure network as outlined above in the claim 25 rejection under 35 U.S.C. 103(a). In addition, a user is prevented from simultaneously connecting to destinations having different security levels (see Boyle, col. 6, lines 15-19).

16. As per claim 34, Boyle covers a secure network as outlined above in the claim 25 rejection under 35 U.S.C. 103(a). Although Boyle discloses that the network security measures of the invention are implemented at the session layer, Boyle also teaches that end-to-end encryption devices conventionally operate at the network layer (see Boyle, col. 2, lines 25-36). Moreover, the invention disclosed by Boyle implements a sealer for encryption and decryption of data for secure transmission and integrity checks (see Boyle, Figure 4A, 'Sealer' and related text). It would be obvious to one of ordinary skill in the art at the time the invention was made to implement security at a network layer of protocol hierarchy. Motivation for such an implementation would enable the invention disclosed by Boyle to provide security services at the network layer and hence provide secure services without having to process the data at higher layers of the hierarchy.

17. As per claim 37, Boyle covers a secure network as outlined above in the claim 25 rejection under 35 U.S.C. 103(a). In addition, the security devices are integrated with the associated host computer (see Boyle, col. 11, lines 24-26).

18. As per claims 38-40, and 44, they are method claims corresponding to claims 25-27, and 31 and they do not teach or define above the information claimed in claims 25-27, and 31. Therefore, claims 38-40, and 44 are rejected as being unpatentable over Boyle in view of Garfinkel for the same reasons set forth in the rejections of claims 25-27, and 31.

19. As per claim 47, it is a method claim corresponding to claims 34 and 38 and it does not teach or define above the information claimed in claims 34 and 38. Therefore, claim 47 is rejected under Boyle in view of Garfinkel for the same reasons set forth in the rejections of claims 34 and 38.

20. As per claim 49, Boyle covers a method as outlined above in the claim 38 rejection under 35 U.S.C. 103(a). In addition, the destination in a user's profile corresponds to a level of security granted to the user (see Boyle, col. 4, lines 60-65; col. 6, lines 15-19; col. 9, lines 38-46).

21. As per claim 59, Boyle covers a secure network as outlined above in the claim 25 rejection under 35 U.S.C. 103(a). Boyle discloses a means to update access control

Art Unit: 2132

information by the network security controller, but does not specify updating user profiles at the network security controller and sending the updated user profiles to the security devices (see Boyle, col. 3, lines 37-39; col. 10, lines 35-37). However, as mentioned above, Boyle does disclose that the secure network is divided into two roles: the security devices implement access control based on policies that include discretionary rules, and the network security controller manages configuration management and security administration for the secure network (see Boyle, col. 4, lines 27-30, 45-49; col. 5, lines 1-7). Furthermore, Boyle teaches that discretionary access rules are based on user identity (see Boyle, col. 5, lines 40-45). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the network covered by Boyle to further comprise the steps of changing user profiles at the network security controller and updating available user profiles at a security device. Motivation for such an implementation would enable the method to perform updates to user profiles at the controller for centralized management of access control to all devices in the secure network.

22. As per claim 69, Boyle covers a method for controlling a sending computer to transmit information to a receiving computer over a computer network as outlined above in the claim 25 rejection under 35 U.S.C. 103(a). In addition, Boyle discloses an embodiment of the invention wherein the security devices are implemented for internetwork connections (routing determination), and hence the security mechanisms to determine whether communication is authorized are implemented at a network layer

of ISO protocol hierarchy (see Figure 2, 'Gateway (SINU)' and 'Bridge (SINU)' and related text). Furthermore, if a receiving computer is not in a transmit list and/or is not consistent with a transmit window by means of discretionary and mandatory access controls, the transmission of information is terminated, otherwise the security device encrypts the information and transmits the encrypted information to the security device of the receiving computer over the computer network (see Boyle, col. 10, line 30-col. 11, line 2; col. 5, lines 33-65; col. 7, lines 43-67).

23. As per claim 70, it is a method claim corresponding to the invention covered in the claim 59 and 69 rejections and it does not teach or define above the information in the invention covered in the claim 59 and 69 rejections. Therefore, claim 70 is rejected under Boyle in view of Garfinkel for the same reasons set forth in the rejections of claims 59 and 69.

24. As per claim 71, Boyle covers a method as outlined above in the claim 69 rejection under 35 U.S.C. 103(a). In addition, the method further comprises the step of auditing the termination of transmission of information at the network security controller (see Boyle, col. 6, lines 34-39; col. 10, lines 39-42; col. 3, lines 15-21).

25. As per claim 74, Boyle covers a method as outlined above in the claim 69 rejection under 35 U.S.C. 103(a). In addition, the security device prevents simultaneous

connection at different security levels established by mandatory access controls (see Boyle, col. 6, lines 7-19; col. 5, lines 54-65).

26. As per claim 85-87, Boyle covers a network as outlined above in the claim 25 rejection under 35 U.S.C. 103(a). In addition, the security devices include means for enabling a plurality of user profiles to be set for a single user (see col. 3, lines 30-42 as modified by Garfinkel, page 22, 2nd paragraph; page 43, first 2 bullets), the plurality of user profiles to be set for a single user is specific to a particular host computer associated with the security device (see Boyle, col. 8, line 56-col. 9, line 4; col. 9, lines 35-45 as modified by Garfinkel, page 23, Table 2-1, file '/etc/passwd'; page 47, Table 3-1, '/etc/group'), and at least one of the plurality of user profiles enables access to a plurality of destinations (see arguments to claim 25 rejection). The aforementioned cover claims 85-87.

27. Claims 28-30, 41-43, 54, 73, 75, and 88-89 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boyle in view of Garfinkel, and further in view of Holden et al. U.S. Patent No. 5,828,832 (hereinafter Holden). As per claim 28, Boyle covers a secure network as outlined above in the claim 25 rejection under 35 U.S.C. 103(a). Boyle does not expressly disclose alternative implementations of the invention wherein the host computer connects to an untrusted destination. Holden discloses a mixed enclave operation in a computer network with multi-level network security wherein the security device is configured to exploit this flexibility of mixed enclave operations (see

Holden, col. 10, lines 59-60). One configuration disclosed by Holden enables a host computer to connect to an untrusted destination wherein the security device does not implement security mechanisms (see Holden, col. 10, lines 64-67). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Holden to the invention of Boyle. Motivation for such an implementation would enable a greater degree of flexibility with secure network host composition in the invention disclosed by Boyle, since this would allow secure hosts to communicate with unsecured hosts and still offer some protection as disclosed by Holden (see Holden, col. 11, lines 2-5).

28. As per claim 29, Boyle covers a secure network as outlined above in the claim 28 rejection under 35 U.S.C. 103(a). In addition, the untrusted line comprises the Internet (see Boyle, Figure 1 as modified by Holden, Figure 1, Reference No. 36).

29. As per claim 30, Boyle covers a secure network as outlined above in the claim 28 rejection under 35 U.S.C. 103(a). In addition, Holden discloses an implementation of the invention wherein a user cannot simultaneously communicate with a trusted destination and an untrusted destination (see Holden, col. 10, lines 60-63).

30. As per claims 41-43, they are method claims corresponding to claims 28-30 and 38, and they do not teach or define above the information claimed in claims 28-30 and

38. Therefore, claims 41-43 are rejected under Boyle in view of Garfinkel and Holden for the same reasons set forth in the rejections of claims 28-30 and 38.

31. As per claim 54, Boyle covers a secure network as outlined above in the claim 29 rejection under 35 U.S.C. 103(a). In addition, the network security controller enables a security officer to generate the plurality of user profiles (see Boyle, col. 3, lines 30-42). Further, data storage devices for temporarily storing data provided by a host computer are inherent features in data processing devices having functions outlined by Boyle (see Boyle, col. 7, lines 43-56). Finally, Boyle discloses a means for transferring data out of the memory space while making the transferred data inaccessible to the host computer (see Boyle, Figures 3A-C; col. 2, lines 46-54; col. 3, lines 3-12; col. 4, lines 40-44). The aforementioned covers claim 54.

32. As per claims 73 and 75, they are method claims corresponding to claims 29-30 and 69 and they do not teach or define above the information claimed in claims 29-30 and 69. Therefore, claims 73 and 75 are rejected under Boyle in view of Garfinkel and Holden for the same reasons set forth in the rejections of claims 29-30 and 69.

33. As per claims 88 and 89, Boyle covers a secure network as outlined above in the claim 54 rejection under 35 U.S.C. 103(a). In addition, at least one of the plurality of user profiles includes a plurality of destinations (see argument of claim 54), and the network security controller enables the security officer to generate different user profiles

at different security devices for a single user (see col. 3, lines 30-42; col. 8, line 56-col. 9, line 4; col. 9, lines 35-45 as modified by Garfinkel, page 22, 2nd paragraph; page 43, first 2 bullets; page 23, Table 2-1, file '/etc/passwd'; page 47, Table 3-1, '/etc/group').

34. Claims 32 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boyle in view of Garfinkel, and further in view of Stallings Cryptography and Network Security 2nd Edition (hereinafter Stallings). As per claim 32, Boyle covers a secure network as outlined above in the claim 25 rejection under 35 U.S.C. 103(a). Boyle is silent on the matter of a user only selecting one profile during a given connection establishment. However, the feature of mapping a user to a single profile at a given time is equivalent to the well-implemented feature of a user securely logging into an account. For example, Stallings teaches how users are authenticated once per session in a Kerberos authentication service (see Stallings, Figure 11.1). By enforcing a policy of mapping a single user to a single profile, user identification and accountability can be more readily enforced. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the invention disclosed by Boyle to only allow a user to select one profile at a time. Motivation for such an implementation would enforce more stringent network connection accountability.

35. As per claim 45, it is a method claim corresponding to claims 32 and 38 and it does not teach or define above the information claimed in claims 32 and 38. Therefore,

claim 45 is rejected under Boyle in view of Garfinkel and Stallings for the same reasons set forth in the rejections of claims 32 and 38.

Conclusion

36. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00-6:00.

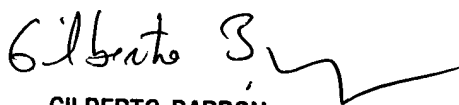
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Jung W Kim
Examiner
Art Unit 2132

Jk
June 3, 2004



GILBERTO BARRÓN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100